Embedding "Least Privilege“ Principles into the AKO Security Model

CIO/G-6 GA&CKO
KM Division

Purpose

- The “Way Ahead” to implement technical and policy solutions to tighten the AKO Security Model.
  - Increase security for AKO Content
  - Implement a more automated default Least Privilege model
  - Enhance group security for sensitive groups (i.e. Foreign Nationals, Foreign Officers) to meet Army requirements

Agenda

- Least Privilege Policy
- AKO Support for Least Privilege
- Gaps in AKO Least Privilege
- Current AKO Public Access Model
- Recommendations
- The Plan
- Next Steps

"Least Privilege" Policy in AR 25-2

- "Least Privilege" refers to how content is managed
  - Correlates with the "Need to Know" principle
  - Configure the least amount of access privilege required for a user to do their job
- Policy existing in AR 25-2:
  - Section 4-5. Minimum Information Assurance requirements
    - "Configure Information Systems (ISs) to implement the principle of least privilege through automated or manual means."
    - "…embed automated security safeguards (when possible) into the design and acquisition of new or updated ISs to ensure a secure infrastructure."

Current AKO Support for "Least Privilege"

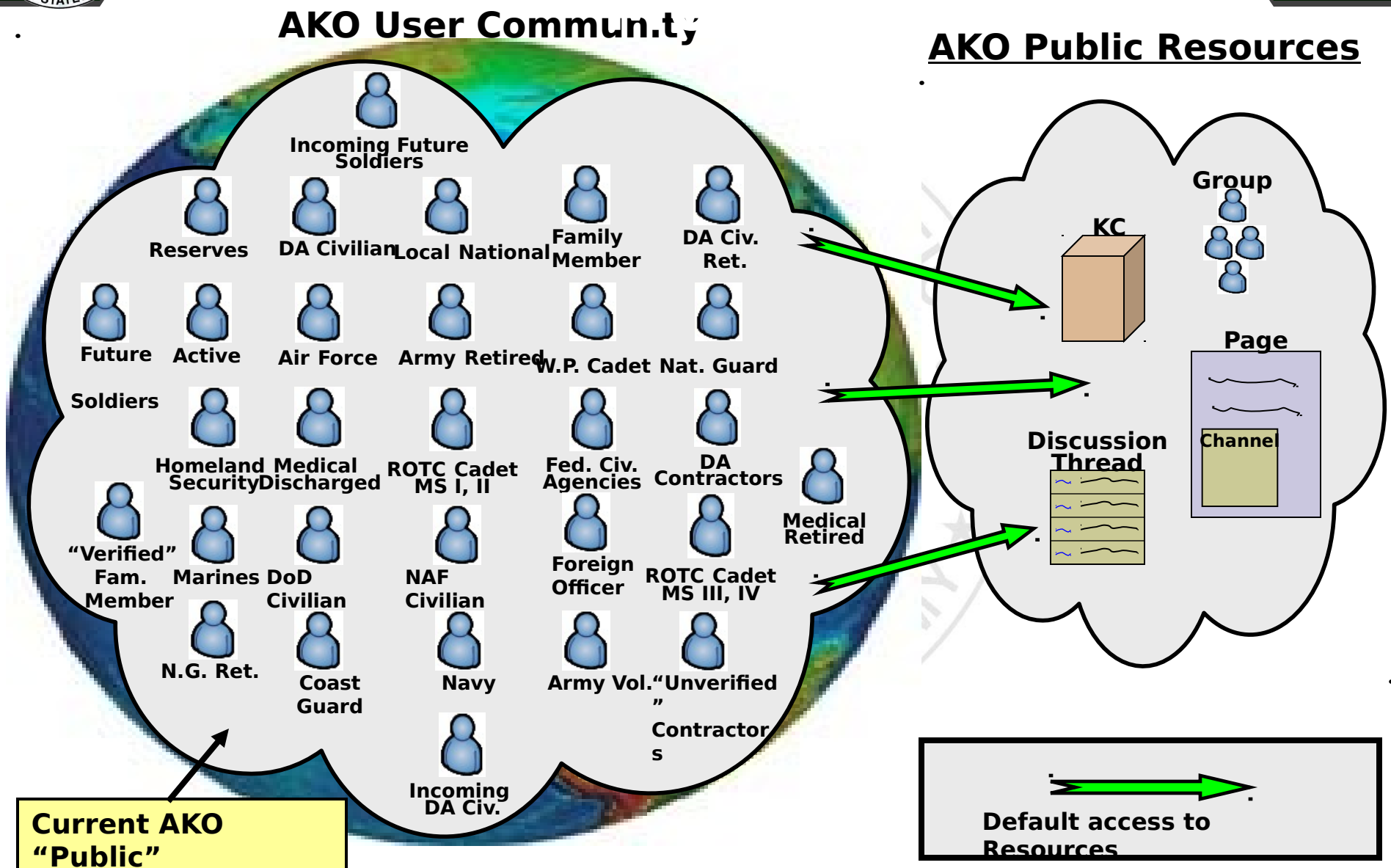
- AKO supports manual configuration of Least Privilege policy
  - Users can limit access privileges to their content using Groups, individual logins, or both
  - Groups offer a scalable manual way to create secure content access
    - Groups IOC in Oct 2004, fully operational Feb 2005
    - Create groups of selected individuals
    - Currently, 30 automated AKO "Army" groups exist based on user roles (i.e. Active Army, DA Civilian, …)
  - Default wizards offer choices to limit access by Groups, such as for a Team

Gaps in AKO "Least Privilege"

- Despite AKO's manual "Least Privilege" capabilities, significant amounts of content are open.
  - There are AKO default security settings which allow all users to view posted content:
    - Within pages – setting called "Public" allows all AKO users to view content
    - Within Knowledge Centers (KC) – setting called "Low" can allow automatic access approval to all AKO users.
- Content which is non-sensitive in itself may become sensitive when data is aggregated.

Restrictions are needed to counter the aggregated access risk.

Current AKO "Public" Access



Proposed Solution

- Technical Solutions
  - Implementation of a more automated Least Privilege model
    - Exploit AKO “Army” groups
  - When possible, “verify” additional AKO “Army” groups (authenticate users against an official DoD data source)
- Governance/Guidance
  - Train content owners to employ groups for access control
  - Require content owners to review and update open content access

“Army” Groups in AKO

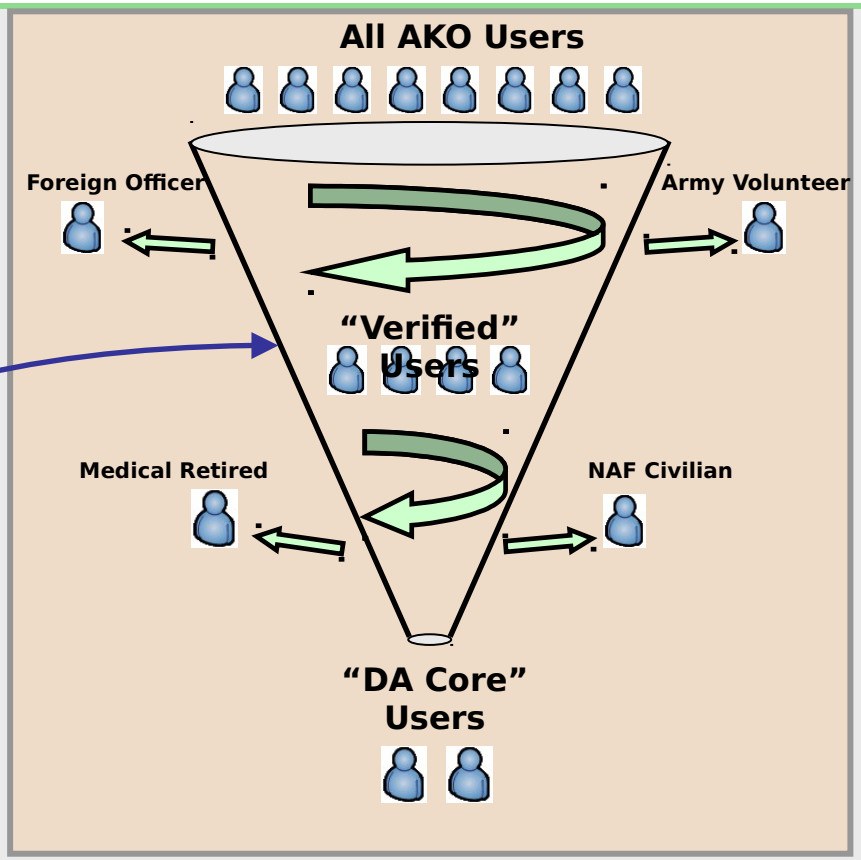
- **Role Based Access Control (RBAC)**
  - Security control system in which users have access to resources based on their roles
- **AKO creates automated groups called “Army” groups**
  - “Army” groups are based on account type
  - Content owners can utilize Army groups for access control
- **“Army” groups, where possible, can be “verified” to add another layer of security**
  - User account information is “verified” by a secondary authoritative DoD data source (ie. DISA, DMDC, ITAPDB, CAC)

Approach for Executing "Least Privilege"

- **Use automated AKO "Army" Groups**
  - "Active Army" and other key groups are "verified"
- **Create a "DA Core" group based on a subset of existing "Army" Groups**
  - Proposed group: Active Army, DA Civilian, Army Reserve, National Guard, DA "verified" Contractors
  - Can provide a RBAC-like capability
- **Use "DA Core" to replace "Public" default settings for new and existing content**

Proposed AKO "DA Core" Role

UNVERIFIED GROUP
%Army Volunteer
Unverified Contractor
DoD Civilian
Family Member of Full AKO Member
Federal Civilian Agencies
Foreign Officer (Attached to U.S. Army)
Homeland Security
Incoming DA Civilian
Incoming Future Soldier
Local National Employee
Medical Discharge
+ROTC Cadets (MS I and II)
US Air Force
US Coast Guard
US Marine Corps
US Navy
VERIFIED GROUP
Active Army*
Army Reserves*
Army Retired
DA Civilian*
DA Civilian, Retired
Future Soldiers
Medical Retired
#NAF Civilian
National Guard*
National Guard, Retired
+ROTC Cadets (MS III and IV)
U.S. Military Academy Cadets
Verified contractors*
Verified Family Members



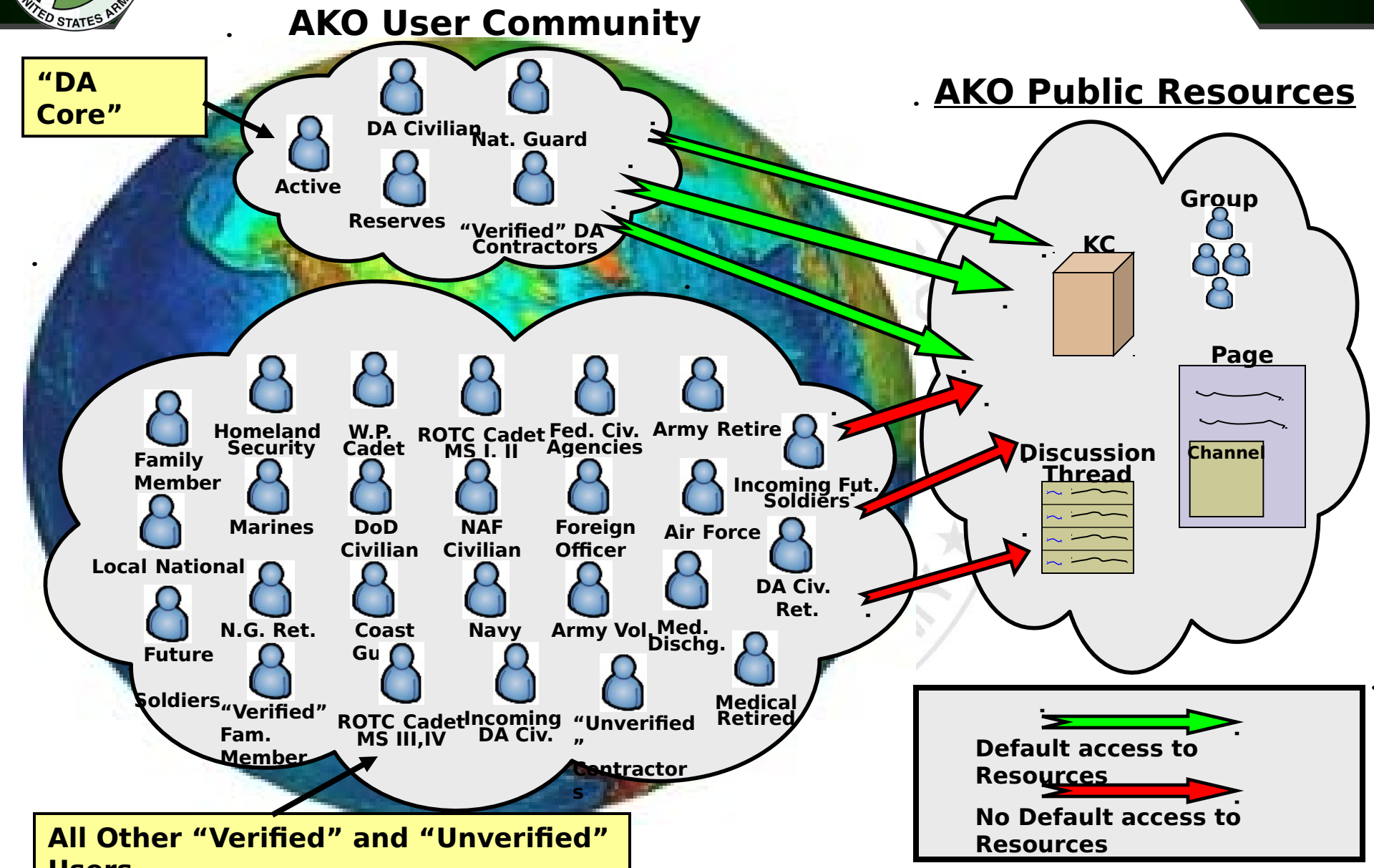
***Groups highlighted in Verified Group are members of proposed "DA Cor**

% Army Volunteer = Personnel supporting the Army's initiatives through volunteer work, etc. who have a direct need to access AKO.

+ ROTC Cadet (MS I & II; MS III & IV) = Scholarship cadets in four Military Science levels for R&D. The accounts for MS III & IV is a full account type while the accounts for MS I & II is a guest account type.

 # NAF Civilian = Employees hired through funding received from sources other than Congressionally appropriated monies.

“Least Privilege” Access Model



Executing "Least Privilege" For New Content

- **Insert "DA Core" group into the content Wizard as the broadest default access choice**
  - Will replace "Public" setting in content Wizard
  - "DA Core" group excludes sensitive groups such as Foreign Officers/Nationals and unverified sponsored accounts
- **Content creators can add access for individuals/groups outside the "DA Core" group as needed**

Impact:
Removes uncontrolled broad access capabilities

Executing "Least Privilege" for Existing Content

- **Replace "Public" setting with "DA Core" for all existing content**
- **Changes access to previous "Public" content for users not in the "DA Core" group**
  - Impact varies by content type
    - **Pages** – users not in "DA Core" permissions will lose default access
    - **KC's** – users not in "DA Core" will lose discoverability privileges unless previously approved for access
  - Content owners must be advised in a planned fashion
- **Will not [illegible] users in DA Core [illegible]**

Result:
Removes uncontrolled broad access capabilities

Plan for Implementing "Least Privilege"

1. Use the AKO Requirements Process to document & manage change
2. AKO PO Review and analysis
3. Develop and implement communication plan, guidance and training for administrators & AKO Help Desk (Educate the AKO user)
4. Reconfigure wizards and “Public” content access

Verifying AKO Users

- Move towards verifying as many AKO users as possible
  - Already verifying many users against ITAPDB and DEERS as well as CAC
  - Search for and link to authoritative DoD databases to verify additional users where possible
  - Integrate verification without system degradation
  - Verification adds an extra layer of security by authenticating that the user is legitimate

Next Steps

- Approve proposed “DA Core” group:
  - Active Army, Army Reserves, National Guard, DA Civilians, DA “verified” contractors
- Approve substitution of “DA Core” group for “Public” group in content security settings

Timeline

- 1 November
  - Begin requirements process based on decision
- 15 November
  - Review requirements and timeline with AKO PO
- Based on requirements review, timeline will be set for development and delivery